COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) IELASI	Membro di designazione rappresentativa degli intermediari
(BO) CAPILLI	Membro di designazione rappresentativa dei clienti

Relatore FEDERICA IELASI

Seduta del 08/10/2024

FATTO

L'istante, anche tramite denuncia allegata al ricorso, disconosce un'operazione di bonifico effettuata tramite *home banking* di importo pari a Euro 9.752,00.

In particolare, parte ricorrente dichiara di essere titolare di un conto corrente presso l'intermediario resistente e di una carta di pagamento ad esso collegato. In data 30 ottobre 2023 l'istante dichiara di essere stato contattato telefonicamente da un numero riconducibile alla resistente. Durante tale telefonata, un sedicente operatore bancario lo invitava a svolgere determinate operazioni per mettere in sicurezza il proprio conto. Nel dettaglio, il sedicente operatore riferiva all'istante di un tentato bonifico dall'estero, per bloccare il quale occorreva seguire le informazioni da lui fornite. Ignaro di quanto stesse accadendo, parte ricorrente decideva di seguire le indicazioni dell'operatore, fornendogli il codice OTP ricevuto sul proprio cellulare. L'istante dichiara di possedere una password, ma di non aver mai fornito le informazioni per l'accesso al proprio conto web. Parte ricorrente dichiara inoltre l'assenza di notifiche nell'App relative ad accessi al proprio conto web, anche se dalla App risultava una geolocalizzazione diversa della sua posizione. A seguito di tale circostanza, resosi conto della frode, parte ricorrente aveva prontamente contattato l'assistenza dell'intermediario. Tuttavia, le richieste di blocco del bonifico e di ulteriori verifiche non hanno avuto alcun riscontro fino alla fine dell'anno. I

messaggi ricevuti sul proprio cellulare provenivano dallo stesso mittente da cui vengono regolarmente inviati dall'intermediario i codici di sicurezza per effettuare le transazioni online. L'istante evidenzia come il grado di sofisticazione della truffa l'ha indotto a credere alla genuinità del messaggio ricevuto, poiché non si evincevano circostanze che lo rendessero dubbio.

Esperito infruttuosamente reclamo, l'istante inoltra ricorso all'ABF, chiedendo la refusione da parte dell'intermediario convenuto dell'importo fraudolentemente sottratto con l'operazione disconosciuta, per un importo pari a Euro 9.752,00.

Convenuta ritualmente, parte resistente chiarisce e controdeduce quanto segue:

- l'operazione di pagamento contestata è stata correttamente autorizzata mediante l'utilizzo di credenziali statiche e dinamiche in possesso del ricorrente con autenticazione forte a due fattori (SCA), registrata e contabilizzata senza aver subito le conseguenze di alcun tipo di malfunzionamento;
- l'accesso all'area riservata del cliente è stato eseguito con username e password scelte dall'utente, oltre all'OTP trasmessa via SMS al numero di cellulare indicato dal cliente in fase di apertura del rapporto;
- è stato successivamente inserito un ordine di bonifico confermato con successivo codice OTP inviato tramite SMS;
- ciò fa emergere l'assenza di diligenza che ha connotato la condotta del ricorrente che verosimilmente ha condiviso le proprie credenziali e il codice OTP ricevuto, come confermato dallo stesso in sede di denuncia;
- il ricorrente ha violato dunque con colpa grave le norme di cui al d.lgs. 11/2010, fornendo ai terzi malfattori i dati necessari per accedere alla propria area riservata, nonché l'OTP, nonostante la banca metta a disposizione dei propri clienti contenuti relativi alla sicurezza informatica;
- il ricorrente ha fornito il codice OTP necessario per autorizzare il bonifico nonostante il testo dell'SMS contenesse informazioni chiare in merito all'operazione da eseguire;
- ad ulteriore conferma della colpa grave del ricorrente, nel caso di specie, la banca aveva inviato una segnalazione via e-mail e via *push* nell'App della disposizione di un ordine di bonifico immediatamente dopo la sua esecuzione;
- l'intermediario ha tentato successivamente di stornare il bonifico, ma lo storno ha avuto esito negativo a causa dell'assenza di fondi, trasferiti al di fuori del conto corrente beneficiario immediatamente dopo l'accredito.

A tali controdeduzioni, parte ricorrente replica specificando che:

- la sottrazione della somma di denaro non è ascrivibile alla condotta del ricorrente bensì alla negligenza dei sistemi informatici della banca;
- il ricorrente è stato infatti contattato dai canali ufficiali della banca;
- non vi è prova di un'effettiva conoscenza dei messaggi *push* nel contesto spazio-temporale nel quale la truffa si stava consumando; il ricorrente potrebbe averli visionati solo al termine dell'iter criminoso;
- nel caso di specie, il ricorrente non ha ricevuto alcun messaggio *push*, altrimenti si sarebbe allarmato e non avrebbe dato seguito a quanto accaduto;
- non ha mai fornito gli accessi al suo conto corrente tramite web e non erano presenti

notifiche nella App di accessi al web;

- spetta alla banca verificare la riconducibilità delle operazioni alla volontà del cliente, impiegando la diligenza dell'accordo banchiere;
- dalle stesse allegazioni di controparte emerge che le comunicazioni non sono arrivate all'indirizzo IP del correntista, ma a un terzo;
- la banca ha l'obbligo di adottare gli accorgimenti adeguati a prevenire l'illecita captazione di dati attraverso il *phishing,* onde evitare accessi non autorizzati;
- se la banca avesse vigilato diligentemente avrebbe dovuto accorgersi degli accessi anomali effettuati sul profilo della vittima; risultava infatti un indirizzo IP mai usato prima dal cliente;
- la mancata attivazione o il malfunzionamento del servizio di *alert* fonda la responsabilità della banca da inadeguata organizzazione;
- i log prodotti dalla banca non valgono a dimostrare la presenza di un sistema di autenticazione forte nel caso in esame.

L'intermediario, nel ribadire quanto affermato in sede di controdeduzioni, controreplica affermando che:

- i log dimostrano chiaramente l'inserimento di credenziali statiche e dinamiche;
- i terzi malfattori sono riusciti a eseguire l'operazione di pagamento oggetto di contestazione grazie alla collaborazione del ricorrente, che ha condiviso con loro le chiavi statiche e l'OTP dinamica.

Sulla base di quanto precede, l'intermediario chiede all'Arbitro di rigettare il ricorso nel merito per infondatezza.

DIRITTO

Le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Ai sensi dell'art. 10 del D.Lgs. 27 gennaio 2010, n. 11, è onere dell'intermediario provare che le operazioni siano state autenticate, correttamente registrate e contabilizzate. In mancanza della suddetta prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute.

Nel caso di specie, parte ricorrente disconosce una sola operazione. Il Collegio ha quindi verificato se con riferimento alla stessa l'intermediario abbia fornito elementi a sostegno della relativa legittimità.

Nella controversia in esame, occorre verificare i passaggi autorizzativi relativi a due attività:

- l'accesso all'*home banking*;
- la transazione disposta online tramite *home banking* (bonifico).

Il Collegio ha in primo luogo proceduto alla verifica della modalità di autenticazione e della conseguente legittimità della prima attività. A tale riguardo, l'intermediario dichiara che per l'accesso all'area riservata, ai sensi dell'art. 10 del Regolamento Delegato (UE) 2018/839, è sempre richiesta l'autenticazione forte mediante OTP, trasmessa via SMS all'utenza mobile indicata dal cliente in fase di apertura del rapporto e validata dalla banca, nei casi di *(a)* primo accesso e *(b)* qualora siano trascorsi più di 90 giorni dall'ultima volta che il cliente ha avuto accesso al conto corrente mediante autenticazione forte. Ove non venga effettuata l'autenticazione forte, l'accesso del cliente è limitato alle seguenti informazioni: saldo del conto corrente; operazioni di pagamento eseguite negli ultimi 90 giorni.

L'intermediario convenuto fornisce in atti documentazione relativa agli accessi all'*home banking*, da cui si evince come l'accesso del 30 ottobre 2023, giorno della frode, sia avvenuto solo tramite username e password, mentre il precedente accesso del 29 settembre 2023 era avvenuto tramite username, password e OTP.

Nel caso di specie, dalla documentazione in atti, emerge dunque che:

- l'accesso all'area riservata con credenziali statiche (username e password) + elemento di possesso (OTP) è stato effettuato più di 30 giorni prima della frode;
- il giorno della frode, l'accesso all'*home banking* è stato effettuato unicamente tramite username e password.

Il giorno della truffa, nella fase di accesso all'*home banking* è stato utilizzato il solo fattore di conoscenza. In merito al secondo fattore di autenticazione, l'intermediario riferisce di essersi avvalso dell'esenzione dalla SCA prevista dall'art. 10 Reg. UE 2018/389 e quindi di non aver richiesto l'autenticazione forte mediante trasmissione via SMS dell'OTP all'utenza mobile indicata dal cliente in fase di apertura del rapporto.

Ai sensi di quanto disposto dal regolatore, l'art. 10 del regolamento delegato di cui sopra dispone sì l'esenzione per la SCA, ma solo ed esclusivamente per l'accesso al conto a fini informativi, non certo anche per quell'accesso che avvenga al fine dell'esecuzione di disposizioni di pagamento (si veda al riguardo Collegio di Bologna, decisione n. 9591/2024, Collegio di Bari, decisione n. 6380/2024).

Alla luce di quanto appena rilevato, l'accesso al conto nel caso di specie – di natura non meramente informativa, perché seguito dalla disposizione di un bonifico – non risulta conforme ai requisiti normativamente previsti.

In ogni caso, in merito alle esenzioni SCA previste dal Reg. Delegato 389/2018, l'EBA ha chiarito che, qualora l'intermediario decida di non adottare l'autenticazione forte, applicando un'esenzione dalla SCA normativamente prevista, nel caso in cui le operazioni vengano disconosciute dal cliente, resta ferma la sua responsabilità (fatta salva la frode dell'utilizzatore) (si veda al riguardo EBA Q&A 2018-4042).

Tale circostanza risulta assorbente rispetto alla verifica delle modalità di autenticazione dell'operazione contestata. La mancanza di autenticazione a doppio fattore nella procedura di accesso all'*home banking* non consente infatti di ritenere provata la regolare autenticazione delle operazioni contestate (a tale riguardo, si vedano, *ex multis*, le seguenti decisioni: Collegio di Bologna, n. 12274/2022; Collegio di Bari, n. 9425/2022 e 2568/2023).

In continuità con l'orientamento condiviso dai Collegi territoriali di questo Arbitro, si

evidenzia come possano essere opposte al titolare della carta di pagamento le operazioni contestate soltanto qualora vi sia l'esibizione (da parte dell'intermediario) di una documentazione che consenta di verificare la corretta autenticazione delle stesse. In aderenza al dato normativo, la prova di autenticazione rappresenta infatti un *prius* logico rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La mancata allegazione della necessaria documentazione atta a dimostrare la corretta autenticazione nella fase di accesso all'*home banking*, rende quindi irrilevante ogni ulteriore valutazione in merito all'autenticazione del bonifico e alla sussistenza o meno della colpa grave in capo all'istante.

La domanda di parte ricorrente merita pertanto accoglimento, con conseguente diritto della stessa alla restituzione di un importo complessivo pari a Euro 9.752,00.

La richiesta di franchigia da parte dell'intermediario convenuto, giunta solo in fase di controrepliche, è da ritenersi tardiva e non può quindi essere accolta.

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 9.752,00 (novemilasettecentocinquantadue/00).

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARCELLO MARINARI